# UNITED STATES PATENT AND TRADEMARK OFFICE

**UNITED STATES DEPARTMENT OF COMMERCE**
**United States Patent and Trademark Office**
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/902,696 | 07/12/2001 | Hirofumi Muratani | 211428US2SRD | 1589 |

22850    7590    05/16/2006

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

| EXAMINER |
|---|
| ABRISHAMKAR, KAVEH |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2131 | |

DATE MAILED: 05/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) ☒ Responsive to communication(s) filed on *24 February 2006*.

2a) ☐ This action is **FINAL**.     2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) ☒ Claim(s) *1-3 and 6-26* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-3 and 6-26* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

       1. ☐ Certified copies of the priority documents have been received.

       2. ☐ Certified copies of the priority documents have been received in Application No. _____.

       3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

1.    A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection.  Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114.  Applicant's submission filed on

February 24, 2006 has been entered.


2.    Claims 1-3, and 6-26 are currently being considered.


### *Response to Arguments*

Applicant's arguments filed February 24, 2006 have been fully considered but

they are not persuasive for the following reasons:

Regarding amended claim 1, the Applicant argues that the CPA, Shimizu et al.

(EP 0982895 A2), does not teach "at least two round processing circuits having third

and fourth round functions, the third round function being an inverse of the second

round function, and the fourth round function being an inverse of the first round

function." This argument is not found persuasive.  The CPA discloses that the key

conversion functions are constructed of involution functions, which are functions that are

their own inverses (column 8 lines 29-39).  Therefore, it is respectfully asserted that the

CPA does disclose the inverse relationships described above, as it discloses that the key conversion functions employ involution functions.

Furthermore, the Applicant argues that the CPA does not teach the sub key output from a round processing circuit of a last stage is a common key. This argument is not found persuasive. The CPA employs involution functions in the key conversion functions so that a relationship between the decryption key and the encryption key is realized (column 8 lines 29-39). This relationship is demonstrated by "a cipher text encrypted by an encryption key can be decrypted by a decryption key, while a cipher text encrypted by a decryption key can be decrypted by an encryption key" (column 4 lines 11-22). This is interpreted as being a common key which is output from the last stage of the of key conversion functions.

Therefore, the rejection of the pending claims is maintained as given below.

## *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

3.      Claims 1-9, 11-18 are rejected under 35 U.S.C. 102(a) as being anticipated by Shimizu et al. (European Patent Application EP0982895).

Regarding claim 1, Shimizu discloses:

An encryption apparatus based on a common key encryption system in which a

plurality of expanded keys are used in a predetermined order in a data randomizing

process for encryption and in a reversed order in a data randomizing process for

decryption, the apparatus comprising:

"*a plurality of round processing circuits connected in series*" (Abstract,

Figure 2, column 4 lines 43-58, column 13 lines 40-45), wherein a plurality of key

transformation functions (processing circuits) are connected in series, "*the round*

*processing circuit of a first stage receiving a common key and subjecting the*

*common key to a round function to output a sub key*" (Figure 2, column 13 lines 27-

45), wherein the key transformation function (processing circuit) take an encryption key

(common key) as an input and via the key transformation functions (round processing

functions) output intermediary keys (sub keys), and "*the round processing circuit of*

*other stages receiving the sub key output from the round processing circuit of a*

*previous stage and subjecting the sub key to a round function to output a sub*

*key, the sub key output from the round processing circuit of a last stage being*

*the common key*" (Figure 2, column 13 lines 27-45), wherein the key transformation

functions which incorporate round functions (round processing circuits) output

intermediary keys (sub keys) which are then subject to another transformation at the

next key transformation circuit to output a next intermediary key (sub key), and the final

key transformation function outputs a decryption key (common key); and

"*a plurality of expanded key generating circuits configured to receive the*

*sub keys output from at least a part of said round processing circuits and output*

*expanded keys based on all or some bits of the received sub keys*" (Figure 6,

column 4 lines 43-53, column 7 lines 38-45, column 8 lines 54-57, column 13 lines 27-

56), wherein there is a transformation function (expanded key generating circuit) which

receives an intermediary key (sub key) and based on the sub key generates an

extended (expanded) key;

wherein "*the plurality of round processing circuits comprise a first portion*

*including at least two round processing circuits having first and second round*

*functions and a second portion which follows the first portion, the second portion*

*including at least two round processing circuits having third and fourth round*

*functions, the third round function being an inverse of the second round function,*

*and the fourth round function being an inverse of the first round function*" (column

3 lines 20-27), wherein the conversion (function) and the inverse conversion (function)

of the different stages are equal by virtue of the involution function employed in the key

generation.


Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Shimizu

discloses:

The encryption apparatus according to claim 1, where said "*plurality of*

*expanded key generating circuits subject all or some bits of the received sub*

*keys to a predetermined conversion processing to output the expanded keys*"

(Figure 6, column 4 lines 43-53, column 7 lines 38-45, column 8 lines 54-57, column 13

lines 27-56), wherein there is a transformation function (expanded key generating

circuit) which receives an intermediary key (sub key) and based on the bits of the sub

key generates an extended (expanded) key by using a transformation function

(conversion processing).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Shimizu

discloses:

The encryption apparatus according to claim 1, wherein "*the round function of

the round processing circuit of i-th stage is an inverse function of the round

function of the round function of the round processing circuit of (j-i+1)-th stage, j

being half of the total number of stages of the round processing circuits and i

being 1 to j*" (column 3 lines 20-27), wherein the conversion (function) and the inverse

conversion (function) of the different stages are equal by virtue of the involution function

employed in the key generation.

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Shimizu

discloses:

The encryption apparatus according to claim 1, further comprising "*a selector

configured to select some of the sub keys output from said plurality of round

processing circuits, the selected sub keys being supplied to said plurality of

expanded key generating circuits*" (Figure 5, column 13 lines 27-56), wherein there is

a selection circuit (selector) configured to received a selection signal and an

intermediary key (sub key), which processes the selected intermediary keys (sub keys)

and provides it to the next key transformation function which takes the input

intermediary key (sub key) provides it to a transformation function (expanding key

generating circuit) which outputs the extended (expanded) key.

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Shimizu

discloses:

The encryption apparatus according to claim 6, wherein said "*selector selects*

*the sub keys output from round processing circuits other than a first group of*

*round processing circuits including the round processing circuit of the first stage*

*and a second group of round processing circuits including the round processing*

*circuit of the last stage*" (Figure 5, column 13 lines 27-56), wherein there is a selection

circuit (selector) configured to received a selection signal and an intermediary key (sub

key), which processes the selected intermediary keys (sub keys) and provides it to the

next key transformation function which takes the input intermediary key (sub key)

provides it to a transformation function (expanding key generating circuit) which outputs

the extended (expanded) key.

Claim 8 is rejected as applied above in rejecting claim 6. Furthermore, Shimizu

discloses:

The encryption apparatus according to claim 6, wherein "*said selector selects one of the sub key output from a round processing circuit of i-th stage and the sub key output from a round processing circuit of (j-i+1)-th stage, j being half of the total number of stages of the round processing circuits and i being 1 to j*" (Figure 5, column 13 lines 27-56), wherein there is a selection circuit (selector) configured to received a selection signal and an intermediary key (sub key), which processes the selected intermediary keys (sub keys) and provides it to the next key transformation function which takes the input intermediary key (sub key) provides it to a transformation function (expanding key generating circuit) which outputs the extended (expanded) key.

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Shimizu discloses:

The encryption apparatus according to claim 1, wherein said "*plurality of expanded key generating circuits change an order of the sub keys generated from said plurality of round processing and generates the expanded keys in a changed order*" (column 4 lines 43-53), wherein the key conversion process can be performed in an order or in another order reverse to the order transferred between the key conversion functions.

Claim 19 is rejected as applied above in rejecting claim 1. Furthermore, Shimizu discloses:

The encryption apparatus according to claim 1, wherein *"the plurality of round processing circuits comprise a first half of round processing circuits and a second half of round processing circuits, a round function of the first half of round processing circuits being inverse to a round function of the second half of round processing circuits"* (column 3 lines 20-27), wherein the conversion (function) and the inverse conversion (function) of the different stages are equal by virtue of the involution function employed in the key generation.

Claim 20 is rejected as applied above in rejecting claim 1. Furthermore, Shimizu discloses:

The encryption apparatus according to claim 1, wherein *"the plurality of round processing circuits comprise a first half of round processing circuits and a second half of round processing circuits, round functions of the first half of round processing circuits being inverse to round functions of the second half of round processing circuits"* (column 3 lines 20-27), wherein the conversion (function) and the inverse conversion (function) of the different stages are equal by virtue of the involution function employed in the key generation.

Claim 21 is rejected as applied above in rejecting claim 1. Furthermore, Shimizu discloses:

The encryption apparatus according to claim 1, wherein *"each of the round processing circuits in the pair of round processing circuit having inverse*

*functions, comprises logic elements and a plurality of output terminals, such that*

*the plurality of output terminals are connected to different logic elements so that*

*different sub keys are output from each output terminal"* (Figures 2-3, column 7

lines 20-34), wherein an intermediary key conversion result is output to produce

ciphertext.

Claim 22 is rejected as applied above in rejecting claim 1. Furthermore, Shimizu

discloses:

The encryption apparatus according to claim 1, wherein *"each of the round*

*processing circuits in the pair of round processing circuits having inverse round*

*functions, comprises corresponding logic elements wherein the logic elements of*

*each round processing circuit are interconnected differently, so as to output*

*different sub keys"* (Figures 2-3, column 7 lines 20-34), wherein an intermediary key

conversion result is output to produce ciphertext.

4.      Claims 11 – 12, and 23-26 are decryption apparatus claims analogous to the

encryption apparatus claims rejected above, as the same key conversion section is

employed in both the encryption and the decryption (column 3 lines 35-43), and

therefore, are rejected following the same reasoning.

5.    Claims 13 – 16 are expanded key generation apparatus claims analogous to the

encryption apparatus claims rejected above, and therefore, are rejected following the

same reasoning.

6.    Claims 17 – 18 are computer-readable medium claims analogous to the

encryption apparatus claims rejected above, and therefore, are rejected following the

same reasoning.

### Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.    Claim 10 is rejected under 35 U.S.C. 103(a) as being obvious over Shimizu et al.

(European Patent Application EP0982895) in view of Leppek (U.S. Patent No.

5,933,501).

Claim 10 is rejected as applied above in rejecting claim 1.  Furthermore, Shimizu

discloses:

The encryption apparatus according to claim 1.  Shimizu does not explicitly

disclose "*plurality of expanded key generating circuits generate the expanded*

*keys in number exceeding the number of expanded keys required for the data*

*randomizing process and output an expanded common key indicating which*

*expanded keys are supplied to the data randomizing process.*" Leppek discloses

an encryption scheme, which uses an address code generator to generate an address

code sequence (expanded common key), which uses the specific sequence to select an

order of encryption operators (encryption keys) to be used in a determined sequence to

encrypt the data (column 4 lines 15-33). Leppek uses such a configuration of using

successively different encryption operators to create an output that has no discernible

encryption footprint (Abstract). Shimizu and Leppek are analogous arts as both deal

with encryption schemes that outline a processing scheme to encrypt and decrypt

information. The sequence selecting function of Leppek can be placed at the output of

the expanded keys and before the function of encrypting the message using the

expanded keys of Shimizu in order to provide a system which selects the different

encryption operator sequences based on a code sequence (expanded common key).

Therefore it would have been obvious to one of ordinary skill in the art to use the

encryption operator sequence selection of Leppek in conjunction with the encryption

processor of Shimizu to provide a system wherein the encrypting sequences are

randomized in order to avoid leaving a encryption footprint.

### *Conclusion*

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-

272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

KA
05/11/2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100